

MATTHEW  
ANDERSON  
NDigitally signed by  
MATTHEW  
ANDERSON  
Date: 2021.05.18  
13:23:07 -05'00'

AO 106 (Rev. 04/010) Application for Search Warrant

AUTHORIZED AND APPROVED/DATE:

UNITED STATES DISTRICT COURT  
for the

WESTERN

DISTRICT OF

OKLAHOMA

In the Matter of the Search of )  
 (Briefly describe the property to be searched )  
 or identify the person by name and address )  
 Information associated with the cellular )  
 device assigned call number (580) 304-3632 )  
 with international mobile subscriber identity )  
 number 31041029766435 in the custody or )  
 control of AT&T Wireless, 11760 U.S. )  
 Highway 1, North Palm Beach, Florida 33408 )

Case No: MJ-21- 303 -SM

## APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following [Person or Property?] (*identify the person or describe property to be searched and give its location*):

See Attachment A, which is incorporated by reference herein.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B, which is incorporated by reference herein.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
 21 U.S.C. § 846

Offense Description  
 Drug Conspiracy

The application is based on these facts:

See attached Affidavit of Task Force Officer Joel Hall, Homeland Security Investigations, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).  
☐ Delayed notice of [No. of Days] days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).



Applicant's signature

Daniel Hunter Marsh  
 Special Agent  
 Federal Bureau of Investigations

Sworn to before me and signed in my presence.

Date: May 18, 2021

City and State: Oklahoma City, Oklahoma

A handwritten signature in blue ink, appearing to read "Suzanne Mitchell", is written over a light blue rectangular background.

*Judge's signature*

Suzanne Mitchell, U.S. Magistrate Judge

*Printed name and title*

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
THE CELLULAR DEVICE ASSIGNED  
CALL NUMBER **(580) 304-3632** WITH  
INTERNATIONAL MOBILE  
SUBSCRIBER IDENTITY NUMBER  
310410297664350 IN THE CUSTODY  
OR CONTROL OF AT&T WIRELESS,  
11760 U.S. HIGHWAY 1, NORTH PALM  
BEACH, FLORIDA 33408

Case No. MJ-21- 303 SM

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Daniel Hunter Marsh, being first duly sworn, hereby depose and  
state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for  
information associated with a certain cellular device assigned with call number **(580)  
304-3632** (the “**Subject Account**”) that is in the custody or control of AT&T Wireless, a  
wireless telephone service provider that accepts process at 11760 U.S. Highway 1, North  
Palm Beach, Florida 33408. The information to be searched is described in the following  
paragraphs and in Attachment A. This affidavit is made in support of an application for a  
search warrant under 18 U.S.C. § 2703(c)(1)(A) to require AT&T Wireless to disclose to  
the government copies of the information further described in Section I of Attachment B.  
Upon receipt of the information described in Section I of Attachment B, government-

authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a federal law enforcement officer within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since February 1, 2009. I am currently assigned to the Oklahoma City Division, Stillwater Resident Agency. My responsibilities include the investigation of possible violations of federal law, including investigation of gang-related criminal activity, violent crime, and drug trafficking. During my career, my investigations have included the use of various surveillance techniques and the execution of various search, seizure, and arrest warrants.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violation of Title 21, United States Code, Section 846 has been committed by Jamie Scott **WILSON**, Ulyssa **FAHS**, Taylor **THOMASON**, Mary **SANCHEZ**, Kade **RICE**, and others. There is probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

5. The Court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

6. The United States, including Federal Bureau of Investigation, Oklahoma City, Oklahoma (“FBI”), is conducting a criminal investigation into the distribution of methamphetamine in the Western District of Oklahoma. **WILSON** and his former girlfriend **FAHS** were identified as part of a conspiracy to possess with the intent to distribute methamphetamine and federally indicted in February 2021 in case number 21-cr-0021-R.

7. On November 16, 2020 the U.S. Customs Border Patrol (CBP) checkpoint station located in the vicinity of Yuma, Arizona contacted DEA Yuma office in reference to a Nissan Rogue being stopped and seized at the checkpoint after an inspection revealed what appeared to be a large quantity of methamphetamine. Occupants of the vehicle included driver, **SANCHEZ**, **THOMASON**, and **RICE**. **THOMASON** is a known relative of **WILSON**. DEA agents arrested the three occupants of the vehicle and seized approximately 70 kilos of methamphetamine located in three large duffle bags in the back of the vehicle. At the time of the arrest, DEA agents attempted to conduct interviews and obtain consent to examine cell phones belonging to the girls. **SANCHEZ** and **RICE** provided consent and **THOMASON** declined. It was later determined through the

interviews and text communications that **THOMASON** was the person who had recruited the other girls to accompany her on the trip. **THOMASON** was also sending communications to **RICE** prior to the trip asking if she had the ability to rent a vehicle.

8. During this time period, **WILSON** is believed to have used the **Subject Account** because: (i) text messages between the **Subject Account** and **THOMASON** reference **WILSON**'s address; (ii) text messages sent from the **Subject Account** refer to **THOMASON** as "niece" and text messages from **THOMASON** to the **Subject Account** refer to the user of the **Subject Account** as "uncle"; (iii) **SANCHEZ** has the name "Jamie" associated with the **Subject Account** in her phone; and (iv) a subpoena was served for toll records related to the **Subject Account** around the time of the Yuma seizure from November 9, 2020, to November 23, 2020, and showed that the **Subject Account** was in contact with numbers belonging to persons identified as associates, friends, or family members of **WILSON**.

9. I have requested subscriber information on the **Subject Account**. The information revealed that the account is a prepaid account that was activated on October 27, 2020. It lists the subscriber name as "Prepaid Customer" and provides a subscriber address of 17330 Preston Road, Dallas, Texas 75252. This address is associated with AT&T Wireless.

10. Based on interviews, cell phone examinations and surveillance video I have concluded that the three occupants left Oklahoma on the morning of Sunday, November 15, 2020, and swapped vehicles into the Nissan Rogue in Ponca City before driving to

Calexico, CA and meeting WILSON at a motel. The following communication was extracted by the DEA Yuma office following a search warrant on the phone belonging to THOMASON. The conversation is between THOMASON's phone and the Subject Account and occurred on November 14, 2020, at approximately 8:04 pm CST:

**Subject Account:** Wat up niece u down to ride I will rent u a car

**THOMASON:** Yesssss

**THOMASON:** Call me

11. On November 15, 2020, the Subject Account exchanged a number of text messages with THOMASON between 8:44 am CST until approximately 12:37 pm CST. On November 15, 2020, WILSON and FAHS lived at 820 South 6th, Ponca City, Oklahoma:

**Subject Account:** 820 south 6that appartment 4

**THOMASON:** Send addy again

**Subject Account:** 820 south 6<sup>th</sup>

**Subject Account:** Appartment 4

**THOMASON:** Got it

**THOMASON:** What's the address uncle

12. On November 16, 2020, the Subject Account and THOMASON exchanged a number of text messages, beginning at approximately 2:30 am CST:

**Subject Account:** 341 E, 4thstreet that is hotel

**THOMASON:** What's the town y'all in

**THOMASON:** So many address pull up when I put that in

**THOMASON:** Did you go past calexico ?

**Subject Account:** [Sent photograph depicting California Motel and Suites]

**THOMASON:** Got it. Still around 7 am

13. On November 16, 2020, the **Subject Account** and **THOMASON** exchanged text messages again, beginning at approximately 8:54 pm CST and ending at approximately 9:50 pm CST:

**Subject Account:** Y'all hurry up and get a 75

**THOMASON:** We coming

**THOMASON:** Are y'all pulled over

**THOMASON:** On the side of the road

**Subject Account:** No we're not we're still driving but we're going to go 65

**THOMASON:** We're stopped man

**THOMASON:** Get ahold of my momma please

14. These last messages corresponded with the arrest of **THOMASON** and the seizure of approximately 70 kilograms of methamphetamine from the Nissan Rogue stopped by CBP in Yuma, Arizona.

15. In my training and experience, I have learned that AT&T Wireless is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the



device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

16. Based on my training and experience, I know that AT&T Wireless can collect cell-site data about the **Subject Account**. I also know that wireless providers such as AT&T Wireless typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

17. Based on my training and experience, I know that wireless providers such as AT&T Wireless typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as AT&T Wireless typically collect and retain information about their subscribers’ use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the


information can be used to identify the **Subject Account**'s user or users and may assist in the identification of co-conspirators and/or victims.

**AUTHORIZATION REQUEST**

18. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

19. I further request that the Court direct AT&T Wireless to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on AT&T Wireless, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



---

DANIEL HUNTER MARSH  
Special Agent  
Federal Bureau of Investigations

Subscribed and sworn to before me on May 18, 2021



---

SUZANNE MITCHELL  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to records and information associated with the cellular telephone assigned call number **(580) 304-3632**, with International Mobile Subscriber Identity Number 310410297664350 (the “**Subject Account**”), that are stored at premises controlled by AT&T Wireless (the “**Provider**”), a wireless telephone service provider that accepts process at 11760 U.S. Highway 1, North Palm Beach, Florida 33408.

**ATTACHMENT B**

**Particular Things to Be Seized**

**I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the **Subject Account** listed in Attachment A:

- a. The following information about the customers or subscribers associated with the **Subject Account** for the time period September 1, 2020, to November 30, 2020:
  - i. Names (including subscriber names, user names, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network

Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);

- vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address);
- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records;
- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the **Subject Account** for the time period from November 10, 2020, to November 30, 2020, including:
  - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
  - ii. information regarding the cell tower and antenna face (also known as “sectors” through which the communication were sent and received.

## **II. Information to be Seized by the Government**

All information described in Section I that constitutes evidence of violations of Title 21, United States Code, Section 846, involving Jamie Wilson, Ulyssa Fahs, Taylor Thomason, Mary Sanchez, and Kade Rice during the period of November 10, 2020, to November 30, 2020.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency

personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things described in this Warrant.